United States
Department of
Agriculture

Office of the
Assistant Secretary
for Administration

1400 Independence
Avenue SW

Washington, DC
20250-0103

JUN 21 2006

TO: All Washington Metropolitan Area Employees

FROM: Boyd K. Rutherford
Assistant Secretary
for Administration

SUBJECT: Urgent Washington Area Employee Notification

This memorandum is to inform Washington Metropolitan Area employees that a USDA computer system has been accessed by an unauthorized third party, and we are investigating the full extent of this breach.

On June 20, 2006, computer forensic examiners briefed me regarding an unauthorized intrusion of USDA computer systems. The examiners verified that the systems had been accessed but could not confirm or deny whether the database had been viewed or downloaded.

The systems in question included a database containing employee names, social security numbers, and photos. Worksite information that is readily available to the public was also contained within the database. Approximately 26,000 current and former Washington, D.C.-based USDA employees and contractors are potentially affected. It is unknown at this time whether personal information was viewed by unauthorized persons.

When the intrusion was originally discovered, a computer security vendor was immediately asked to review the systems and concluded that the security software protected the personal identity information. A subsequent request was made for a USDA computer forensic specialist, as well as the Office of Inspector General, to analyze the hard disk drives of the impacted systems and determine the extent of the intrusion.

USDA is doing all that it can to safeguard its data systems and inform potentially impacted employees of this event. Within the next week, all impacted employees will receive a letter notifying them of what additional measures they can take to protect themselves. USDA has created a web site that includes valuable information on steps to be taken if you suspect personal identity theft. The website may be accessed at www.usda.gov/oo/beprepared/identity. People who believe they may be affected by the data breach can go to www.firstgov.gov for more information.

USDA will also provide free credit monitoring services to potentially affected employees for a period of 12 months. Details of the credit monitoring program will be made available in the coming days.

We regret that this incident occurred. We are fully committed to ensuring the security of USDA data as well as equipping our employees, retirees, and contractors with the tools necessary to minimize the impact of this intrusion. We have established an incident hotline that is available by dialing 1 (800) FED-INFO (333-4636), Monday through Saturday between the hours of 8:00 a.m., and 9:00 p.m., Eastern Daylight Savings Time.

What happened, and how does it affect me?

What happened?

Over the June 3, 2006, weekend, USDA cyber security staffers monitoring our systems detected some suspicious activity involving an Office of Operations workstation and two servers containing employee personal data. The indication was that someone from outside of USDA was attempting to gain unauthorized access to the system.

What information was included in the affected system?

The data stored in the system includes an individual's name, social security number, employing agency photo, and internal building location.

The system in question does not host any USDA health records or any financial information.

How do I know if information about me was stolen?

At this point, it is unknown whether any employee's personal information has been accessed or compromised. However, letters are being sent to the employees, contractors, and retirees whose information was in the affected system. Because this involves approximately 26,000 individuals, the letters will be sent over a period of about two weeks.

What is USDA doing to assist employees whose personal identity information might have been viewed by unauthorized persons?

USDA will provide free credit monitoring services to potentially affected employees for a period of twelve months. A follow-up letter will be sent to these employees to explain credit monitoring and outline enrollment procedures.

What should I do?

What should I do to protect myself? Do I have to close my bank account or cancel my credit cards?

USDA is encouraging all employees to be vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions, and to immediately report any suspicious or unusual activity local law enforcement officials and the Federal Trade Commission (see "What should I do if I detect a problem with any of my accounts?" below.)

For tips on how to guard against misuse of personal information, visit the Federal Trade Commission website at http://www.ftc.gov/.

One way to monitor your financial accounts is to review your credit report. By law you are entitled to one free credit report each year. Request a free credit report from one of the three major credit bureaus – Equifax, Experian, TransUnion – at www.AnnualCreditReport.com or by calling 1-877-322-8228.

What do you mean by "suspicious activity"?

Suspicious activities could include the following:

- Inquiries from companies you haven't contacted or done business with
- Purchases or charges on your accounts you didn't make
- New accounts you didn't open or changes to existing accounts you didn't make
- Bills that don't arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you didn't make

What is identity theft?

Identity theft occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes.

I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?

USDA strongly recommends that individuals closely monitor their financial statements and review the guidelines provided on the USDA "Be Prepared" web page (www.usda.gov/oo/beprepared/identify.html).

If there was a security breach, what is the earliest date at which suspicious activity might have occurred?

The attempted breach occurred over the weekend of June 2-4, 2006. If any data was accessed and misused, it is likely that suspicious activity would be noticeable beginning in the month of June.

What should I do if I detect a problem with any of my accounts?

The Federal Trade Commission recommends the following **four** steps if you detect suspicious activity:

Step 1 – **Contact the fraud department of one of the three major credit bureaus:**

- Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, Texas 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Step 2 – **Close any accounts that have been tampered with or opened fraudulently.**

Step 3 – **File a police report with your local police or the police in the community where the identity theft took place.**

Step 4 – **File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline:**

- By telephone: 1-877-438-4338
- Online at www.consumer.gov/idtheft
- By mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

Where can I get more information?

Please check the USDA "Be Prepared" web site at www.usda.gov/oo/beprepared/identify.html.

People who believe they may be affected by the data breach can go to www.firstgov.gov for more information.

What are my remedies if my identity is stolen and used illegally?

The Federal Trade Commission has produced a booklet to help you remedy the effects of an identity theft. It describes what steps to take, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future. The contents of the booklet, *Taking Charge: Fighting Back Against Identity Theft*, are available online at http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

Can Social Security put a flag on my number?

No, unlike the credit bureaus, the Social Security Administration (SSA) cannot put a flag or security alert of any type on your Social Security number.

To report that someone is using your Social Security number, file a complaint with the Federal Trade Commission by using the four steps outlined above:

- Internet: www.consumer.gov/idtheft
- Telephone: 1-877-IDTHEFT (1-877-438-4338)

Can I get a new Social Security number?

SSA will not issue you a new Social Security number as a precaution. SSA assigns a new Social Security number in rare cases, and only if the number holder provides evidence that the old number has been used with criminal or harmful intent and that the misuse has caused the number holder to be subjected to recent economic or personal hardship.

How do I file a police report?

Individuals who are victims of actual identity theft should file a local police report about the incident. The Federal Trade Commission advises consumers who are victims of identity theft to get a copy of the police report or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. You should also retain for your records a copy of the USDA memo regarding the potential breach.

Information about steps to take if you are a victim of identity theft is available online at www.consumer.gov or by calling the Federal Trade Commission at 1-877-IDTHEFT (1-877-438-4338).

What if the local police won't take a report?

In order to file a police report, you must show you have suffered an actual identity theft or harm due to fraudulent activity or misuse of account information.

If you have experienced identity theft or harm, the Federal Trade Commission (FTC) suggests providing as much documentation as you can to prove your case, including debt collection reports, credit reports, or other evidence of fraudulent activity.

Information about steps to take if you are a victim of identity theft is available online at www.consumer.gov or by calling the Federal Trade Commission at 1-877-IDTHEFT (1-877-438-4338).

The FTC also suggests being persistent if local authorities tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute.

The FTC advises that if you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead. If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police. Some states require the police to take reports for identity theft. Check with the office of your State Attorney General www.naag.org to find out if your state has this law.